REMARKS

Claims 1-23 are pending with claims 1 and 18 being independent. Claims 1, 7, 10, 11, 12, 13, 16, 17, 18, and 23 have been amended. The support for amending the claims can be found at least on paragraphs [0013], [0015], [0020], [0021], [0023], [0025], [0054], [0056], [0058-[0062], [0068]-[0070], [0073], [0078], [0089]-[0098], [0100], [0102]-[0105], and FIG. 2.

In light of foregoing amendment and following remarks, reconsideration and allowance of all pending claims are respectfully requested.

Rejections Under 35 U.S.C. § 112

Claims 1 and 23 stand rejected under 35 U.S.C. § 112, 2nd ¶ for allegedly being indefinite. While not agreeing with the rejections, claims have been amended to obviate the rejections.

Rejections Under 35 U.S.C. § 103(a)

Claims 1-6 and 8-23 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent Application Publication No. 2003/0225596 to Richardson et al. ("Richardson") in view of U.S. Patent No. 6,788,997 to ("Frederick").

Claim 1 and its dependent claims

Claim 1 is amended. Reads as follows:

1. A computerised identity matching management process for the supply of a pharmaceutical substance to an authorised patient, the process comprising the steps of:

identifying a patient who is requesting the supply of the substance, comprising the steps of:

a management computer receiving a request, from capture apparatus waiting to commence a biometric capture process representative of the patient to initiate the capture process;

the management computer responding to the request to return a message to the capture apparatus at a first time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process;

the management computer, after returning the message, receiving a captured biometric representative of the patient from the capture apparatus coded with the code, at a second time; and

the management computer operating, when the second time is less than a predetermined time later than the first time, to decode the captured biometric and initiate a matching process to find a match for the decoded captured biometric against stored biometric records and to retrieve an identification code representative of the patient when a match is found;

retrieving a date stamp and using the identification code to retrieve a stored data record of the patient which includes at least a substance the patient is prescribed, a quantity in which the substance is to be supplied and a date at which the substance is to be supplied;

determining whether the date stamp matches the date at which the substance is to be supplied, and

if a match is determined, supplying the substance in the prescribed quantity and recording information to form a record to update the supply of the substance to the patient.

Thus, claim 1 is directed to dispensing pharmaceutical substance such as methadone directly to authorized patients for whom the pharmaceutical substance has been prescribed by a health care practitioner for the treatment of opioid dependence, for example. To properly dispense the pharmaceutical substance, the claimed method recites an identity matching management process for the supply of a pharmaceutical substance to the authorised patient. The patient is authorized because the heal care practitioner, the prescriber, has prescribed the pharmaceutical substance to the patient.

To determine whether the patient is an authorized patient, the claimed method recites "a management computer receiving a request, from capture apparatus waiting to commence a biometric capture process representative of the patient to initiate the capture process." For example, a prisoner who is on a methadone treatment program can present himself at a clinic in prison and undergo a retinal scan, corneal scan, or other type of biometric scan. The result of that scan can be compared with the contents of a database which contains biometric data for patients who are authorized to receive the requested pharmaceutical substance for methadone treatment, for example. If the scanned biometric matches with a stored biometric, the patient receives the dosage of methadone which is authorized for that patient.

In contrast to claim 1, Richardson is concerned with the access to medications, by a nurse or the like, in a locked storage cabinet or depot. In Richardson, an electronic accessory, such as a key ring, card, badge or the like is fastened to the healthcare worker who is authorized for access to that storage. The electronic accessory in Richardson comprises a biomedical identification. In Richardson, a biometric scan is taken of the healthcare worker and compared with the biometric data which is associated with the electronic accessory. It is important to note that in Richardson, the identity of the key holder is verified by comparing the scanned biometric with the biometric which is associated with the electronic accessory (see Richardson at ¶ [0012]).

> According to another aspect of the invention, the identity of the key holder is quickly verified because only one file is compared to the biometric scan instead of comparing a biometric scan to a library of files to identify an individual being scanned. The present invention provides a one-to-one matching of biometric identification, requiring less time than a one-to-many identification process.

Thus, Richardson does not describe the claimed "initiate a matching process to find a match for the decoded captured biometric against stored biometric records and to retrieve an identification code representative of the patient when a match is found." In other words, Richardson is limited to comparing the scanned biometric data with the data in the key holder, a single record, which cannot reasonably be construed as the claimed stored biometric records. Because of this difference, Richardson is merely checking to determine if the health care provider is wearing the proper hey holder. To properly identify a patient as the authorized patient, the process recited in claim 1 requires comparing the scanned biometric data against stored records that includes a list of authorized patients.

Moreover, in the environment of the claimed process, it is not feasible to provide the patient with any form of token (such as a key ring or card) because of the certitude of fraud arising in the use of such devices. It is even less feasible to rely on the issue of a PIN or other identifier to the patients, requiring the patient to enter the PIN and undergo biometric scan. The overall patient identification process according to the claimed process actually takes less time than would be taken by the process of Richardson. Richardson would require the patient to produce a token of some sort, insert that token into the apparatus, the conducting of a biometric scan of the patient, and then performing a one-to-one biometric identification. The time taken according to Richardson would be greater than would be the process according to the claimed process, namely, the time taken for conducting the biometric scan and conducting a one-to-many identification process.

Also, Richardson fails to teach or suggest the claimed "the management computer responding to the request to return a message to the capture apparatus at a first time, the message containing a unique code, and where receipt of the message containing the code at the capture apparatus causes initiation of the capture process; the management computer, after returning the message, receiving a captured biometric representative of the patient from the capture apparatus coded with the code, at a second time the management computer operating, when the second time is less than a predetermined time later than the first time, to decode the captured biometric

and initiate a matching process to find a match for the decoded captured biometric against stored biometric records and to retrieve an identification code representative of the patient when a match is found." The claimed unique code is used to encode or encrypt the captured biometric data of the patient, and the claimed management computer is able to decode the biometric data only if "the second time is less than a predetermined time later than the first time." This guarantees that the unique code used to encode or encrypt the biometric data is still valid to be decoded.

In contrast to claim 1, Richardson does not use the claimed unique code to encode the captured biometric data of the patient. While the Office contends that paragraphs [0028], [0030], [0057], and [0058] allegedly teach the limitations, the cited portions of Richardson fail to support the contention.

For example, paragraphs [0028], [0030], [0057] and [0058] in Richardson describe an electronic identification key port 124 that receives information from an electronic identification key 128 carried by the user. The electronic identification key in Richardson stores "information…[that] relates to the identification of the key holder/user." Thus, in Richardson, the information that relates to the identification of the key holder/user is provided from the electronic identification key to the medical storage depot 100. However, claim 1 recites that "the management computer respond[s] to the request to return a message to the capture apparatus at a first time, the message containing a unique code." The electronic identification key in Richardson cannot reasonably be construed as the claimed management computer at least because the electronic identification key is not responding to a message from the storage depot. Also, in Richardson, the information received from the electronic identification key is not used to encode the captured biometric image or send the captured biometric image to the electronic identification key. Moreover, the electronic identification key in Richardson does not decode any data or message received from the storage depot "when the second time is less than a predetermined time later than the first time." These deficiencies in Richardson may be due to the fact that Richardson is not concerned with encrypting the captured biometric data. In contrast to claim 1, the electronic identification key is used to verify that the user is a valid user.

The addition of Frederick fails to alleviate the deficiencies of Richardson. Frederick describes a system for monitoring and dispensing medical items (see Frederick at Abstract). In Frederick, a medical technician logs into the system, searches for patient information and obtains medicine appropriate for a particular patient (see Frederick at 15: 63-16:55).

> …a medical technician who wishes to operate the system and remove medical items from the hook registers 10 operates 65 the display terminal. The terminal screen outputs a visual prompt for the user to identify himself or herself to the system by input of identifying data....Upon further use of the display terminal, the user may access certain information about patients, procedures or physicians which is stored in records in the data store of the computer 84…

(Id.).

Similar to Richardson, the system in Frederick is to provide health care workers with access to medications. Also, Frederick does not obtain biometric data as described in claim 1. Moreover, Frederick does not use a unique code to encode any data let alone the claimed biometric data of the patient. Because the system in Frederick allows the technician to search the patient information and obtain the medication for the patients, there is no need to capture the claimed biometric data or to encode and decode the captured biometric data in Frederick.

In fact, the Office cites to Frederick to merely contend that Frederic teaches the claimed limitations related to "date stamp" (see Office Action Dated June 23, 2009 at 4-5). However, Frederick fails to support even these contentions. Claim 1 does not recite a generic date stamp but rather recites "retrieving a date stamp and using the identification code to retrieve a stored data record of the patient which includes at least a substance the patient is prescribed, a quantity in which the substance is to be supplied and a date at which the substance is to be supplied; determining whether the date stamp matches the date at which the substance is to be supplied, and if a match is determined, supplying the substance in the prescribed quantity and recording information to form a record to update the supply of the substance to the patient." Thus, claim 1 requires retrieving the date stamp **and** using the identification code [received if a match is found] to retrieve a stored data record of the patient. Moreover, the claimed date stamp is used as a trigger to determine if the required substance should be supplied to the patient.

In contrast to claim 1, Frederick describes an order delivery date for delivering medication that was ordered by the system (see Frederick at 10:21-43). The delivery date in Frederick cannot reasonably be construed as the claimed date stamp at least because the date of delivery in Frederick is for an order to be delivered to the medical facility rather than for the system to deliver the medicine to the patient.

For at least these reasons, the proposed combination of Richardson and Frederick fails to teach or suggest each and every limitation of claim 1. Claims 2-6 and 8-17 depend from claim 1 and are patentable over the proposed combination for at least the same reasons.

Claim 18 and its dependent claims

Claim 18 and its dependent claims 19-23 are patentable over the proposed combination of Richardson and Frederick for at least the same reasons.

Rejections Under 35 U.S.C. § 103(a) Based on Richardson, Frederic and Meadows

Claim 7 stand rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Richardson in view of Frederick and further in view of U.S. Patent Application Publication No. 2002/0116390 to Meadows ("Meadows").

Claim 7 depends from claim 1 and is patentable over the proposed combination of Richardson and Frederick for at least reasons similar to claim 1. The addition of Meadows fails to alleviate the deficiencies of Richardson and Frederick.

In contrast to claims 1 and 7, Meadows teaches a system and method for identification and retrieval of lost pets such as dogs (see Meadows at Abstract). The system in Meadows is used to obtain an accurate noseprint of pets and assigns an identification number to the pet (see id.) However, Meadows suffers from the same deficiencies of Richardson and Frederick, namely, the claimed limitations directed to identifying an authorized patient by capturing biometric information from the authorized patient, using an unique code to encode and decode the captured biometric information and retrieving the date stamp to supply the substance to the authorized patient. In fact, the Office cites to Meadows to merely contend that Meadows teaches taking a noseprint picture of a dog (see Office Action Dated June 23, 2009 at pages 7-8).

For at least these reasons, the proposed combination of Richardson, Frederick and Meadows fails to teach or suggest each and every limitation of claims 1 and 7.

CONCLUSION

The foregoing comments made with respect to the positions taken by the Examiner are not to be construed as acquiescence with other positions of the Examiner that have not been explicitly contested. Accordingly, the above arguments for patentability of a claim should not be construed as implying that there are not other valid reasons for patentability of that claim or other claims.

No fees are believed due. Please apply any other charges or credits to Deposit Account 06-1050.

Respectfully submitted,

Date: September 21, 2009

/Hwa C. Lee/
Hwa C. Lee
Reg. No. 59,747

Fish & Richardson P.C.
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (877) 769-7945

HCL/jhg
10942687.doc